A Preliminary Review of Cyber-Deception Factors: Offerings from a Systematic Review

Anoushka P.A. Anderson, Jo Bryce, Carol A. Ireland,[*] Jane L. Ireland

ABSTRACT

The current paper aims to provide a preliminary exploration of the characteristics associated with cyber-deception, by focusing on motivations for engagement and the psychological characteristics of those perpetrating such behaviour. It aims to further outline gaps in the literature and suggest what areas any potential model of cyber-deception could include to benefit future research. A systematic search of 11 databases was undertaken, with additional manual searching for relevant journals and sources. This was followed by data extraction and thematic analysis. A total of 21 studies were identified as meeting eligibility criteria. Six motivational themes emerged (i.e. acquiring attention and sympathy; a response to negative childhood experiences; preserving identity and presenting your 'true' self; to cause intentional harm and to pursue personal enjoyment; to exploit materially; deception as a stress-reliever in response to life strain), and one individual theme (i.e. perpetrator personality). Perpetrator motivation included a varied range of factors, with more static characteristics (i.e. personality) less well captured in the literature. Future research could determine if psychological differences are of value or if the area is better understood through consideration of more dynamic (motivational) factors.

Key words: Cyber-detection; Motivation; Attention; Preserve identity; Harm; Enjoyment

INTRODUCTION

Deception is defined as a deliberate act with the intent to mislead (Buller & Burgoon, 1996), with online deception the use of Information and Communication Technology (ICT) to commit such acts (McGuire &

[*] Corresponding author: CAIreland@uclan.ac.uk

Dowling, 2013) and thus captured using the term cyber-deception. There is recognition that such behaviours can be used for dissocial purposes and that use of ICT can facilitate increased prevalence of this (McGuire & Dowling, 2013), creating a wider range of opportunities for dissocial behaviour (Danquah & Longe, 2011; MacEwan, 2013).

Information on the prevalence rates of cyber-deception is, however, limited and it has been argued that it fails to provide a full account of both perpetration and victimisation (McGuire & Dowling, 2013). This is likely a result of the research being focused on a narrow set of dissocial behaviours, such as fraud. There has been a failure to examine the broader spectrum of deceptive activities that can occur and the differing levels of severity. Regarding reported prevalence rates, Kaakinen, Keipi, Rasanen and Oksanen (2018) found that self-reported rates of victimisation was low, with only 6.4% of a sample of 3,557 users acknowledging victimisation. Yet, 29% of internet users admitted to lying online (Caspi & Gorsky, 2006) suggesting some disparity perhaps in the definition; for example, some may not have recognised lying to represent a form of dissocial behaviour.

The internet is considered, however, a prime medium for deceit (Hancock & Woodworth, 2013), with a reported belief that online deception occurs frequently (Tsikerdekis, 2014). The research does not, however, capture the type of cyber-deception in depth. It could be, for example, that certain types of online lies (e.g. about age) occur more frequently than others, and may be localised more within certain online platforms (e.g. dating websites). There is some evidence for the context being important, with Drouin, Miller, Wehle & Hernandez (2016) reporting dating websites as platforms where users can deceive others regarding career and weight.

Berg, Dickhaut and McCabe (1995) argued that the assumption that cyber-deception is widespread minimises the repercussions of the behaviour because 'everyone does it'. Hancock and Woodworth (2013) further argue that this view results in certain types of cyber-deception being both accepted and expected online. This arguably normalises deceptive activities and reduces the degree to which behaviour is considered dissocial (Suler, 2004).

Historically, the literature that has examined cyber-deception has focused on the individual psychological characteristics of those involved

as opposed to considering contextual and motivational factors. Motivation may be particularly important. Ekman (1997), in considering off-line deception, identified a range of motivations for lying; namely to avoid punishment; to obtain a reward; to protect others; to protect the self from harm; to win the admiration of others; to get out of an awkward social situation; to avoid embarrassment; to maintain privacy; and to exercise power over others. The extent to which these motivations could apply to cyber-deception is unknown and yet may be of value in determining whether or not deception (off-line) and cyber-deception are distinct or shared behaviours that simply use a different medium of enactment. Understanding motivating factors is also of value in formulating a model for cyber-deception that could assist with educating perpetrators, victims, cyber providers and potentially assisting with intervention.

The decision to engage in deceptive behaviour often depends on a balance between reward, cost and successful outcome (Tsikerdekis & Zeadally, 2014). This fits with *Incentive theory*, which suggests that individuals are motivated to engage in deceptive behaviour to achieve rewards such as financial gain or gifts, or to satisfy needs or wants, such as attention (Beckmann & Heckhausen, 2018). The extent to which this applies to cyber-deception remains, however, unknown. This absence of application also applies to research exploring psychological factors of value. In the off-line environment, personality has been found to represent an associated facture. Kashy and DePaulo (1996), for example, found that those who lie frequently scored higher on measures of machiavellianism and psychopathy. A direct link between lying and factors of manipulation, selfishness, callous behaviour, and low levels of remorse was also discovered. Personality factors also linked to victimisation, with Ngo and Paternoster (2011) demonstrating a connection between poor self-control and becoming a victim of deceit. This preliminary review aims to begin exploration of the area of cyber-deception, focusing on the characteristics and motivations of perpetrators in the first instance. In doing so, it aims to outline what is known about causation and motivations for cyber-deception and explore what is known about the psychological characteristics of perpetrators of cyber-deceit.

METHOD

Search strategy

Bibliographic databases were searched via EBSCO Host (Academic Search Complete; Computers and Applied Sciences Complete; Criminal Justice Abstracts; E-Journals; Medline; PsycArticles; PsycInfo; Social Sciences Abstracts, SocIndex; Psychology Database) and Science Direct; Taylor and Francis; Wiley Online; and Web of Science. There was also manual searching of websites that specialise in cyber-deception (e.g. government websites, iPredator.com) and of magazines focusing on cyber-deception (i.e. Cyber Security Source magazine). The following key words were used and combined to search the databases:

1. (deception OR lie* OR lying OR deceit* OR fak*)
2. (online OR internet OR web OR cyber OR virtual community)
3. (malinger* OR crim*)
4. (spam* AND malware AND virus)
5. 1 AND 2 AND 3
6. 1 AND 2 AND 3 AND NOT 4

Inclusion criteria

Studies were considered eligible if they reported information on the aetiology, motivation, characteristics and/or risk-factors for participating in cyber-deception (regardless of whether or not it was described as a criminal act), or discussed how social factors, personality traits and/or psychological disorders influenced the likelihood of an individual participating in cyber-deception. Studies had to be available in English. A date range of 2000 to 2017 was utilised to allow for the identification of sufficient literature, whilst also identifying that papers pre-2000 were not capturing cyber-deception has understood in more recent years.

Exclusion criteria

Studies were excluded if they involved organised cybercrime targeted at IT systems and not individuals (e.g. targeted at businesses); if they involved clear criminal activity (e.g. child abuse or dark-web activities) since the current study was focusing on cyber-deception and not cyber-crime per se.

Eligibility screening

Paper titles were originally screened to determine whether they met the inclusion criteria. If their inclusion was not clear it proceeded to abstract review regardless. All resulting papers were then considered for full-text review. All papers were also quality assessed using an adapted checklist originally designed for completing audits **(**National Institute for Health and Clinical Excellence, 2009), prior to proceeding to full-text analysis. The developed checklist is indicated in Figure 1.

Figure 1: Quality Checklist

Section 1: theoretical approach		
1.1 Is the study clear in what it seeks to do? *For example:* • Is the purpose of the study discussed – aims/objectives/research question(s)? • Is there adequate/appropriate reference to the literature? • Are underpinning values/assumptions/theory discussed?	Clear Unclear Mixed	Comments:
Section 2: study design		
2.1 How defensible/rigorous is the research design/methodology? *For example:* • Is the design appropriate to the research question?	Defensible Not defensible Not sure	Comments:
Section 3: validity		

3.1 Is the role of the researcher clearly described? *For example:* • Does the paper describe the research was explained and presented to the participants?	Clear Unclear Not described	Comments:
3.2 Is the context clearly described? *For example:* • Were observations made in a sufficient variety of circumstances? • Was context bias considered?	Clear Unclear Not sure	Comments:
3.3 Were the methods reliable? • Are the methods adopted reliable? • Do the methods investigate what they claim to?	Reliable Unreliable Not sure	Comments:
Section 4: analysis		
4.1 Is the data analysis sufficiently rigorous? *For example:* • Is the procedure explicit? • Is the procedure reliable/dependable? • Is it clear how the themes and concepts were derived from the data?	Rigorous Not rigorous Not sure/not reported	Comments:
4.2 Are the data 'rich'? *For example:* • How well are the contexts of the data described? • Has the diversity of perspective and content been explored?	Rich Poor Not sure/not reported	Comments:

4.3 Is the analysis reliable? *For example:* • Were discrepant results addressed or ignored?	Reliable Unreliable Not sure/not reported	Comments:
4.4 Are the findings convincing? *For example:* • Are the findings clearly presented? • Are the data appropriately referenced? • Is the reporting clear and coherent?	Convincing Not convincing Not sure	Comments:
4.5 Are the findings relevant to the aims of the study?	Relevant Irrelevant Partially relevant	Comments:
4.6 Are the conclusions adequate?	Adequate Inadequate Not sure	Comments:
Overall assessment		
As far as can be ascertained from the paper, how well was the study conducted? (see guidance notes)		

Source: Quality checklist (slightly abridged). See https://www.nice.org.uk/process/pmg4/chapter/appendix-h-quality-appraisal-checklist-qualitative-studies#checklist-2

Data extraction: Coding

Themes were identified initially by using line-by-line coding, where a potential theme was given a code and then the description of this code was revisited as further papers were considered. The most frequently occurring

codes were then used to group into categories (focus coding). This was a fluid process that required constant revision until all potential coding was considered exhausted and thus saturation was reached. Thematic analysis was the final stage of coding. It used the recommendations of Braun and Clarke (2006) regarding such analysis. It was completed using a coding and qualitative data analysis system (CAQDAS) program, in this instance, ATLAS.ti. An independent reviewer then verified the final coding, after being presented with three randomised papers, to ensure reliability of coding.

RESULTS

Study selection

The final sample comprised 21 papers, with the process of selection listed in Figure 2. The included papers are listed in Figure 3.

Figure 2: Steps of systematic review

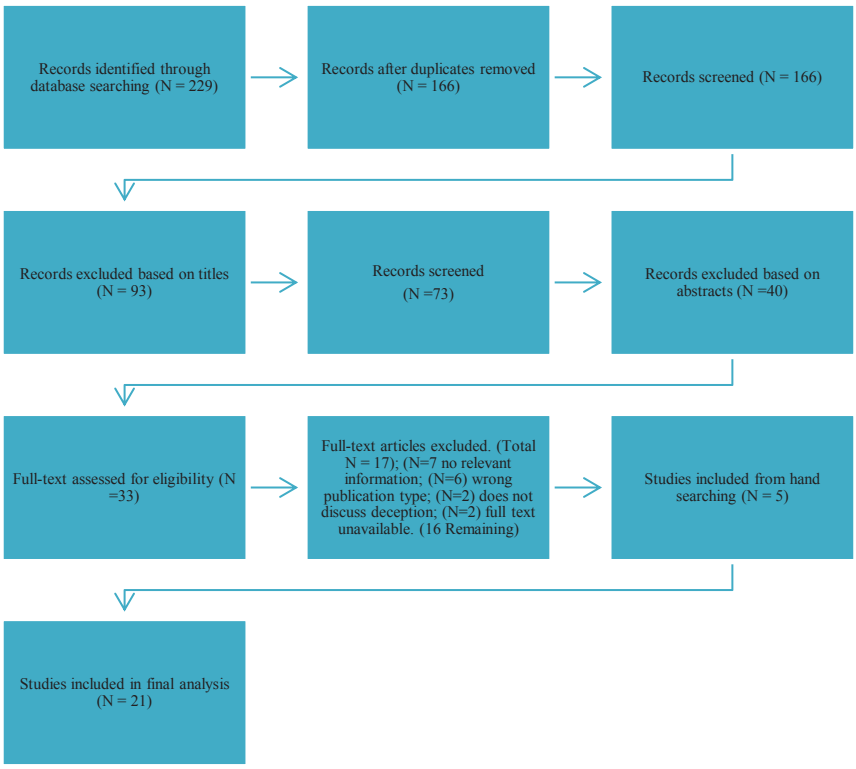

Figure 3. Included studies

Carlson, J. R., George, J. F., Burgoon, J. K., Adkins, M., & White, C. H. (2004). Deception in computer-mediated communication: Group decision and negotiation. *Journal of Computer-Mediated Research*, *13*, 5-28.

Caspi, A., & Gorksy, P. (2006). Online deception: Prevalence, motivation and emotion. *Cyberpsychology and Behaviour*, *9*, 54-62.

Chen, C., & Huang, L. (2011). Online deception investigation: Content analysis and cross-cultural comparison. *International Journal of Business and Information*, *6*, 91-111.

Cunningham, J. M., & Feldman, M. D. (2011). Munchausen by internet: Current perspectives and three new cases. *Psychosomatics*, *52*, 185-189.

Danquah, P., & Longe, O. (2011). Cyber-deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact*, *11*, *169*-182. Retrieved from http://www.jiti.net/v11/jiti.v11n3.169-182.pdf

Feldman, M. D. (2000). Munchausen by internet: Detecting factitious illness and crisis on the internet. *Southern Medical Journal*, *93*, 669-672.

Grazioli, S., & Jarvenpaa, S. L. (2003). Deceived: Under target online. *Communications of the ACM*, *46*, 196-203.

Joinson, A. N., & Dietz-Uhler, B. (2002). Explanations for the perpetration of and reactions to deception in a virtual community. *Social Science Computer Review*, *20*, 275-289.

Kaakinen, M., Keipi, T., Rasanen, P., & Oksanen, A. (2018). Cybercrime victimisation and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults.
Cyberpsychology, Behaviour and Social Networking, *21*, 129–137.

Lawlor, A., & Kirakowski, J. (2014). When the lie is the truth: Grounded theory analysis of an online support group for factitious

disorder. *Psychiatry Research*, *218*, 209-218. doi: 10.1016/j.psychres.2014.03.034

Lawlor, A., & Kirakowski, J. (2017). Claiming someone else's pain: A grounded theory analysis of online community participants experiences of Munchausen by internet. *Computers in Human Behaviour*, *74*, 101-111.

MacEwan, N. (2013). A tricky situation: Deception in cyberspace. *Journal of Criminal Law*, *77*, 417-432.

Moore, P. (2012). The stranger among us: Identity deception in online communities of choice. *Unpublished manuscript.*

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass*, *8*, 388-396.

Stanton, K., Ellickson-Larew, S., & Watson, D. (2016). Development and validation of a measure of online deception and intimacy. *Personality and Individual Differences*, *88*, 187-196. doi: 10.1016/j.paid.2015.09.015

Tskierdekis, M. Z. S. (2014). Online deception in social media. *Communications of the ACM*, *57*, 72-80.

Utz, S. (2005). Types of deception and underlying motivation. *Social Science Computer Review*, *23*, 49-56.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behaviour and social networking*, *21*, 105 – 109.

Whitty, M. T. & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behaviour and Social Networking*, *15*, 22-31.

Whitty, M, T., & Gavin, J. (2001). Age/sex/location: Uncovering the social cues in the development of online relationships. *Cyberpsychology, behaviour and social networking*, *4*, 623–630.

Zhou, L., & Zhang, D. (2008). Following linguistic footprints: Automatic deception detection in online communication. *Communications of the ACM*. Retrieved from http://dl.acm.org/citation.cfm?id=1389972.

Summary focus of the studies

Five papers provided information on the causation of deception; six outlined motivations of participating in cyber-deception; five papers provided information on psychological factors relating to perpetrators of cyber-deception and five papers discussed psychological factors relating to victims of cyber-deception. Findings regarding victims are not included in the themes indicated later since focus is on perpetrators.

Emerging themes

A total of six motivational themes for perpetration were found, with one relating to perpetrator characteristics. These were as follows:

Theme one (motivation): Acquiring attention and sympathy.

This was defined as wanting to elicit feelings of pity, sorrow, admiration, care or to feel noticed. Lawlor and Kirakowski (2014) found that attention and sympathy was the highest perceived motivation for why someone would create a false online persona. Of their respondents, 20% stated they believed users created fake identities to receive attention from others. Some examples of these behaviours were lying about physical or mental health or being part of an exclusive group (e.g. mothers of children with terminal diseases). A theme of coping was also indicated, with it suggested it could be a means of coping with a genuine psychiatric illness (Lawlor and Kirakowski, 2014) and/or to gain support for life pressures, including mental health. There was a suggestion of needing to gain sympathy for the latter, with physical illness more likely to obtain a caring response from others, and thus leading to the fabrication of a physical illness to fulfil psychological needs of care, sympathy and social attention.

The latter was not always identified as a motivation, certainly not one that was immediately conscious (Feldman, 2000), although there was a lack of consistency on this point, with others arguing that the motivation for attention was an explicit one (Lawlor and Kirakowski, 2017). The same study found that participants who feigned illnesses online enjoyed the concern that was shown to them, and it would encourage further deceptive

activities. There was, overall, an indication that the cyber-deception was either masking undisclosed issues or was a means of acquiring unmet psychological needs.

Theme two (motivation): In response to negative childhood experiences.

This was defined as a response to the long-term impacts of experiencing adverse events in childhood. Experiences such as emotional abuse, living in foster care, absentee fathers, physical abuse, irresponsible parenting and sickness were included (Chen & Haung, 2012; Lawlor and Kirakowski, 2017). Some individuals were thought to be attempting to fulfil deficits in interpersonal interaction and what was not available to them emotionally during childhood through cyber-deception.

Theme three (motivation): Preserving identity and presenting your 'true' self.

This was perhaps best described as lying to self-promote, preserve a reputation and/or allow for an individual's 'true' self to be exposed (Joinson & Dietz-Uhler, 2002). It could involve use of an online persona as a means of expressing an individuals 'true' self whilst protected from the social exposure or a need to confirm socially (Joinson & Dietz -Uhler, 2002). This included a need to communicate deviant behaviour without fear of social retribution. Zhou and Zhang (2008) highlighted the role of online communication in relieving individuals of contextual restrictions and formalities, perhaps also supported by an expectation that individuals lie online. This arguably allowed permission for the behaviour and makes it safer. It also allowed individuals to form close connections online (McKenna, Green & Gleason, 2002), particularly for those who were socially anxious who subsequently found expression online a safer experience through cyber-deception.

Theme four (motivation): To cause intentional harm and to pursue personal enjoyment

This included a desire to intentionally cause harm or control a situation for selfish reasons and/or enjoyment. Individuals motivated by a malicious intent were considered unpredictable, with their target group unspecified (Seiter, 2007). It appeared to include 'trolling' (Dynel, 2016). Malice as a primary motivation was, however, was argued to be uncommon (Utz, 2005), and likely promoted by the success of their actions, such as not being prevented by others (Caspi & Gorksy, 2006). Cyber-deception in this

theme was not considered linked with negative emotions such as guilt or shame, but rather enjoyment (Caspi and Gorsky, 2006).

Manipulation was also felt to be a key factor in successfully creating a fake persona (MacEwan, 2013), where a perpetrator was able to exploit the emotions of a victim in the manner intended. Manipulation was described more as a skill, however, than a motivation, and in essence was felt to be the skill that allowed the motivation to be successfully pursued (MacEwan, 2013; Moore 2012).

Theme five (motivation): To exploit materially

This was defined as participating in acts of deception with the aim of benefitting financially or by gaining material goods. Grazioli and Jarvenpaa (2003), for example, found that most acts instigated by material exploitation were motivated by greed, desperation and the need for quick gratification. However, Danquah and Longe (2011) showed that, in some instances, cyber-deceit is a by-product of poor economic status, with perpetrators needing to gather money or goods through cyber-deception. Alternatively, Lawlor and Kirakowski (2017) found that material exploitation was a consequence of cyber-deception rather than a motivating factor, with only 4% of individuals reporting this as a primary motivation for their deceit, with other motivations (e.g. attention and sympathy) more important. Whilst material exploitation may not be the initial reason for cyber-deception, it may become a primary reason as the relationship with the victim(s) evolves.

Theme six (motivation): Deception as a stress-reliever in response to life strain

This was defined as a psychological state that can result from external stressors, which occur when an individual is involved in multiple, high-strain roles such as being a caregiver, home-owner and working in a demanding career (Carlson, George, Burgoon, Adkins & White, 2014). Carlson *et al*. (2014) hypothesised that, when an individual is faced with various external stressors, deception can become a stress-relieving mechanism. The same research argued that when an individual becomes overwhelmed by different role demands, particularly those in the work environment, they need to find an outlet for the negative emotions that accrue. Creating a false online reality can assist with this, with the act of

cyber-deception serving to further reinforce the behaviour and leading to a potential escalation of the deceit (Carlson *et al*, 2014).

Theme seven (individual characteristic): perpetrator personality

This was the only theme identified under the perpetrator category, defined as personality traits, which included lower levels of agreeableness (Stanton, Ellickson-Larew & Watson, 2016) and conscientiousness among perpetrators (Stanton *et al*, 2016; Youli & Chao, 2015), which could link to a tendency to display selfish behaviour, a lack of empathy and maladaptive personality traits (Stanton *et al*, 2016), including psychopathy (Youli & Chao, 2015). Higher levels of neuroticism were also noted in perpetrators (Stanton *et al*, 2015).

DISCUSSION

The current study reported a range of motivations, which appear relevant to cyber-deception. These include a need to acquire attention and sympathy; a response to negative childhood experiences; preserving identity and presenting your 'true' self; to cause intentional harm and to pursue personal enjoyment; to exploit materially; and deception as a stress-reliever in response to life strain. Only a single perpetrator theme emerged, that of personality, with this factor consistent with prior research in the off-line environment (Kashy & DePaulo, 1996). The study further highlighted the limitations in this area, with the noted motivations of descriptive value but the overlap between them and the process by which they were acquired were not captured. This is undoubtedly a product of the research being cross-sectional and not yet advancing its methodology to capture longitudinal design. In short, it highlights the value of motivations in terms of how heterogeneous the perpetrators may be but it does not inform us on how these motivations develop over time and what skills are acquired to enhance their use.

Nevertheless, it demonstrates the importance of motivation, sharing similarities in this regard with the off-line deception literature (Ekman, 1997), particularly in relation to such deception being motivated by a reward, gain (e.g. through manipulation), or by presenting yourself in a manner that accrues admiration. However, this is where the similarities seem to end, with the cyber-deception area not outlining motivations connected to punishment avoidance, protection or to avoid something unpleasant. These related to the off-line context only. It would appear

therefore that the cyber context is focused *more* on coping and the acquisition of attention and sympathy as additional factors of note. Both clearly fit with Incentive Theory, in that there can be motivations of both gain and/or of needs being satisfied (Beckmann & Heckhausen, 2018), but it would appear that the latter is associated more with cyber-deception.

There is, undoubtedly, evidence from the systematic literature review of motivations having a dynamic component to them; for example, material exploitation appeared in some cases a by-product of another original motivation that then developed into a primary motivation across time. What is particularly surprising, however, is the absence of focus on the individual psychological characteristics of the individuals engaging in cyber-deception (Stanton *et al*, 2016; Youli & Chao, 2015). The research at most is presenting a rudimentary analysis of personality but not significantly beyond five-factor considerations of this concept.

The concept of cyber-deception being a potentially dynamic and evolving process is a key offering from the current review, and one that could inform future model development. It certainly fits with prior research that explores the role of decision-making (a dynamic process in its own right) (Tsikerdekis & Zeadally, 2014). A recurrent theme was one of cyber-deception presenting as a result of *accumulating* strains, such as work, other life pressures, and social/individual challenges (e.g. perceived inadequacies, poor mental health), which then evolve into a more sustained pattern of engagement with others on-line. It is the development of this pattern and how the 'relationship' with those they are deceiving that then becomes of interest but as of yet is not captured within the literature. There also appears to be a distinction emerging between those who are engaging in such deception for enjoyment and honing their manipulation skills to do this, versus those that are engaging in cyber-deception in order to cope with the actual or perceived inadequacies in their life (e.g. economic stress, family and personal stress, health stress). It could be speculated that the former (i.e. enjoyment/manipulation motivation) may be related more with unhelpful and damaging personality traits as opposed to the latter (i.e. coping motivations), which may be characterised more by poor coping and inadequacy. The research has yet to offer any insights into this and yet it does suggest that we may require a dynamic model of understanding cyber-deception, one that describes the different pathways through which an individual may emerge as likely to engage in such behaviour.

The role of the environment in driving cyber-deception appears to be emerging as a potential factor but as yet is under-considered and at most is focusing on cumulative stress (i.e. strain) through role-demands and economic hardship. It supports the suggestion that the context in which cyber-deception is occurring is an important one (Drouin *et al*, 2016). What is clearly being evidenced, however, is that this is a dynamic process as opposed to one focusing on individual characteristics. Even personality, although noted as such a characteristic, cannot be enacted in the absence of contact with others; personality is by its very nature a social factor. Consequently, the finding that personality is emerging as valuable could arguably represent a further artefact of the social and thus dynamic environment. It could be speculated that through the medium of the cyberworld opportunities for engagement with others are simply increasing (Danquah & Longe, 2011; MacEwan, 2013), allowing for personality traits to manifest themselves to a now online as opposed to purely direct audience. For example, the notion that cyber-deception is common place, normalised and thus an excusable behaviour (Berg, Dickhaut & McCabe, 1995; Hancock & Woodworth, 2013; Suler, 2004) may be particularly meaningful to those whose personality aligns itself more with exploitation and/or a lack of empathy.

This current study is not without its limitations. It is a preliminary study, with a limited pool of scientific literature on the topic from which to draw its conclusions from. Of the research that it did have available it was cross-sectional and descriptive. This does not lend itself to developing a detailed of understanding concerning the factors involved in making the decision to engage in cyber-deception. Understanding the dynamic process underpinning this decision and, potentially, the individual characteristics that could further reinforce this process, represents an important consideration for future research. A dynamic model that captures what facilitates and inhibits the decision to engagement in cyber-deception and what maintains the engagement is perhaps a key area for consideration as we advance towards proposing a future model to inform education, prevention and intervention.

ABOUT THE AUTHORS

Anoushka Anderson was a student at the University of Central Lancashire, who completed her MSc in Forensic Psychology, and engaged in further post-graduate research, of which the current paper is part of this.

Jo Bryce is Director of the Cyberspace Research Unit at the University of Central Lancashire. Her research interests focus on the psychological, social and forensic aspects of the Internet and related technologies, with a specific focus on their use by young people, associated risk exposure and esafety. Other interests include: the role of ICTs in the commission of criminal offences; online privacy and security; online piracy and filesharing. She is also School equality and diversity lead and Vice-chair of the ethics committee in the school.

Carol A. Ireland PhD, MBA is a Chartered Psychologist, Consultant Forensic Psychologist and Chartered Scientist. She previously worked in a High Secure Setting for nine years, where she was lead for sex offender therapies and critical incident (hostage) negotiation, and where she acted as an advisor in crisis/conflict situations. Dr. Ireland is also a Senior Research Lead at the Ashworth Research Centre at Ashworth Hospital. She also works at CCATS (www.ccats.org.uk), a child and adult therapeutic service in the community. She has more than 70 publications, including journal articles, books and book chapters, mainly on offending, consultancy and crisis (hostage) negotiation.

Jane L. Ireland PhD is a Chartered Forensic Psychologist and Chartered Scientist. Professor Ireland holds a Professorial Chair at the University of Central Lancashire and is a Violence Treatment Lead within High Secure Services, Ashworth Hospital, Mersey Care NHS Trust, where she holds a clinical practice. She is an elected Academy Fellow of the Council of the Academy of Social Sciences and Fellow of the International Society for Research on Aggression (ISRA). Professor Ireland is currently lead for the Ashworth Research Centre (ARC), an NHS clinical and forensic centre for research based within Mersey Care NHS Trust and covers all secure services. Professor Ireland has over 100 publications, including book chapters and journal articles.

REFERENCES

Beckmann, J., & Heckhausen, H. (2018). Motivation as a function of expectancy and incentive. In J. Heckhausen & H. Heckhausen (Eds.), Motivation and Action Cham, Switzerland: Springer, pp. 10-22.

Berg, J., Dickhaut, J., & McCabe, K. (1995). Trust, reciprocity, and social history. *Games and Economic Behaviour*, 10, 122-142.

Braun, V. & Clarke, V. (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2). 77-101. ISSN 1478-0887. Retrieved from http://eprints.uwe.ac.uk/11735

Buller, D., & Burgoon, J. (2006). Interpersonal deception theory. *Communication Theory*, 6, 203-242.

Carlson, J. R., George, J. F., Burgoon, J. K., Adkins, M., & White, C. H. (2004). Deception in computer-mediated communication: Group decision and negotiation. *Journal of Computer-Mediated Research*, 13, 5-28.

Caspi, A., & Gorksy, P. (2006). Online deception: Prevalence, motivation and emotion. *Cyberpsychology and Behaviour*, 9, 54-62.

Chen, C., & Huang, L. (2011). Online deception investigation: Content analysis and cross-cultural comparison. *International Journal of Business and Information*, 6, 91-111.

Danquah, P., & Longe, O. (2011). Cyber-deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. Journal of Information *Technology Impact*, 11, 169-182. Retrieved from http://www.jiti.net/v11/jiti.v11n3.169-182.pdf

Drouin, M., Miller, D., Wehle, S., & Hernandez, E. (2016). Why do people lie online? "Because everyone lies on the internet". *Computers in Human Behaviour*, 64, 134-142.

Dynel, M. (2016). Trolling is not stupid: Internet trolling as the art of deception serving entertainment. Intercultural pragmatics, 13, 3.

Ekman, P. (1997). Deception, lying and demeanour. In D. F. Halpen & A. E. Voiskounsky (Eds.), States of mind: American and post-Soviet perspective on contemporary issues in psychology. Oxford, England: Oxford University Press, pp. 92-105.

Feldman, M. D. (2000). Munchausen by internet: Detecting factitious illness and crisis on the internet. *Southern Medical Journal*, 93, 669-672.

Grazioli, S., & Jarvenpaa, S. L. (2003). Deceived: Under target online. *Communications of the ACM*, 46, 196-203.

Hancock, J. T., Woodworth, M. T., & Porter, S. (2013). Hungry like the wolf: A word-pattern analysis of the language of psychopaths. *Legal and Criminological Psychology*, 181, 102-114.

Joinson, A. N., & Dietz-Uhler, B. (2002). Explanations for the perpetration of and reactions to deception in a virtual community. *Social Science Computer Review,* 20, 275-289.

Kaakinen, M., Keipi, T., Rasanen, P., & Oksanen, A. (2018). Cybercrime victimisation and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behaviour and Social Networking*, 21, 129–137.

Kashy, D. A., & DePaulo, B. M. (1996). Who lies? *Journal of Personality and Social Psychology*, 70, 1037.

Lawlor, A., & Kirakowski, J. (2014). When the lie is the truth: Grounded theory analysis of an online support group for factitious disorder. *Psychiatry Research*, 218, 209-218.

Lawlor, A., & Kirakowski, J. (2017). Claiming someone else's pain: A grounded theory analysis of online community participants experiences of Munchausen by internet. *Computers in Human Behaviour*, 74, 101-111.

MacEwan, N. (2013). A tricky situation: Deception in cyberspace. *Journal of Criminal Law,* 77, 417-432.

McGuire, M., & Dowling, S. (2013). Cyber-crime: A review of the evidence. Home Office Research Report, 75, 1-25.

McKenna, K., Green, A., & Gleason, M. (2002). Relationship formation on the internet: What's the big attraction? *Journal of Social Issues,* 58, 9–31.

Moore, P. (2012). The stranger among us: Identity deception in online communities of choice. Unpublished manuscript.

Ngo, F., & Paternoster, R. (2011). Cybercrime victimisation: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5, 773-793.

Stanton, K., Ellickson-Larew, S., & Watson, D. (2016). Development and validation of a measure of online deception and intimacy. *Personality and Individual Differences*, 88, 187-196.

Suler, J. (2004). The online disinhibition effects. Cyberpsychology and Behaviour, 7, 321-330.

Tskierdekis, M. Z. S. (2014). Online deception in social media. *Communications of the ACM,* 57, 72-80.

Utz, S. (2005). Types of deception and underlying motivation. *Social Science Computer Review,* 23, 49-56.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behaviour and social networking*, 21, 105 – 109.

Whitty, M. T. & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behaviour and Social Networking,* 15, 22-31.

Whitty, M, T., & Gavin, J. (2001). Age/sex/location: Uncovering the social cues in the development of online relationships. *Cyberpsychology, behaviour and social networking*, 4, 623–630.

Youli, H., & Chao, L. (2015). A comparative study between the Dark Triad of personality and the Big Five. *Canadian Social Science,* 11, 93-98.

Zhou, L., & Zhang, D. (2008). Following linguistic footprints: Automatic deception detection in online communication. Communications of the ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1389972.